Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (cancelled)

Claim 2 (cancelled)

Claim 3 (cancelled)

Claim 4 (cancelled)

Claim 5 (cancelled)

Claim 6 (cancelled)

Claim 7 (cancelled)

Claim 8 (cancelled)

Claim 9 (cancelled)

Claim 10 (cancelled)

Claim 11 (cancelled)

Claim 12 (cancelled)

Claim 13 (cancelled)

Claim 14 (cancelled)

Claim 15 (cancelled)

Claim 16 (cancelled)

Claim 17 (previously amended)

Claim 18 (cancelled)

Claim 19 (cancelled)

Claim 20 (cancelled)

Claim 21 (cancelled)

Claim 22 (previously added)

Claim 23 (previously added)

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12. (Cancelled)

13. (Cancelled)

14. (Cancelled)

15. (Cancelled)

16. (Cancelled)

17. (Previously amended)

A computer program product on a computer usable medium for maintaining a secure electronic data search system for a third party electronic data repository in which electronic data file documents are stored in encrypted form in the data repository to prevent access by the repository administrator such a system having a record listing document access privileges for each computer with access to electronic data stored in the repository the program product comprising:

software for updating a manifest for an electronic data file document stored in the repository;

software for identifying all computers with access to the electronic data file

document and for changing such access in an update software for communicating

the change in access to all affected computers;

software for updating access privileges records in all affected software; and

software for communicating the access privilege records to the affected

computers;

software in a vault of the document originator to encrypt a document that it

receives from the originator, prior to forwarding it onto the electric data vault of the

repository;

software in a vault of the repository administrator which on receipt of the

encrypted document, signs the encrypted document itself before storing the

document in the electronic data repository and returns to the originator's vault proof

of deposition of the encrypted document;

software in a vault of a requesting user to request the repository's vault for

use of the requested document;

software in the repository's vault to retrieve a copy of the document in

encrypted form which is forwarded, along with the requester's identity, to the

originator's vault;

software in the originator's vault to verify that the requester is authorized to

view the document from the access control list using an access control list

identifying access ownership privileges for the document stored in the vault itself;

software in the originator's vault when the requester has access to decrypt the

document and forward the decrypted document directly to the requester's vault; and

software in the requester's vault to provide proof of receipt of the decrypted

document wherein the originators of the electronic data files, users of the electronic

data files and the repository administrator all have vaults which are secure extensions of their respective work space.

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Previously added)

A process for maintaining a secure electronic data search system for a third party electronic data repository which contains document data files encrypted to make them secure from the administrator of the repository, the system having a manifest listing access controls for each electronic data file stored in the data repository and a record maintained by a documents originator listing document access privileges for each computer with access to the electronic data stored in the repository which record is maintained secure from the administrator of the repository, the process comprising the steps performed by the documents originator of:

updating a manifest for an electronic data file stored in the repository;

identifying all computers with a change in access to the electronic data file effected by the update;

updating the access privileges records of all affected computers;

communicating the updated access privilege records to the affected computers;

providing the originators of the electronic data files, users of the electronic data files and the repository with vaults which are secure extensions of their respective work spaces;

encrypting in the vault of the document originator a document of the originator, prior to forwarding it on to the vault of the repository;

signing the encrypted document in the vault of the repository before storing the document in the electronic repository and returning to the originator's vault proof of deposition of the encrypted document;

sending from the vault of a requesting user to the repository's vault a request to use the requested document;

retrieving from the repository's vault a copy of the document in encrypted form and forwarding it along with the requester's identity, to the originator's vault;

verifying in the originator's vault that the requester is authorized to view the document from the access control list in the originators vault identifying access privileges for the document;

decrypting the document in the originator's vault when the requester has access and forwarding the decrypted document directly to the requester's vault; and

having the requester's vault provide proof of receipt of the decrypted document.

23. (Previously added)

A computer program product on a computer usable medium for maintaining a secure electronic data search system for a third party electronic data repository in which electronic data file documents are stored in encrypted form in the data repository to prevent access by the repository administrator such a system having a manifest to an electronic data document secure to the originator of the electronic document listing document access privileges for each computer with access to the electronic data document stored in the repository, the program product comprising:

software for updating the manifest for the electronic data file document stored in the repository;

software for identifying all computers with access to the electronic data file document and for changing such access in an update software for communicating the change in access to all affected computers;

software in the vault of the document originator to encrypt a document that it receives from the originator, prior to forwarding it on to the vault of the repository administrator;

software in the vault of the repository which on receipt of the encrypted document, signs the encrypted document before storing the document in the electronic repository and returning to the originator's vault proof of deposition of the encrypted document;

software in the vault of a requesting user to the repository's vault to request use of the requested document;

software in repository's vault to retrieve a copy of the document in encrypted form which is forwarded, along with the requester's identity, to the originator's vault;

software in the originator's vault to verify that the requester is authorized to view the document using an access control list identifying access ownership privileges for the document stored in the vault itself;

software in the originator's vault when the requester has access decrypts the document and forwards the decrypted document directly to the requester's vault; and

software in the requester's vault to provide proof of receipt of the decrypted document.